Enumeration

Course Introduction

Alexis Ahmed

Senior Penetration Tester @HackerSploit
Offensive Security Instructor @INE

Course Topic Overview

- Introduction to Enumeration
- The Nmap Scripting Engine (NSE)
- Service Enumeration
- Service Enumeration with Nmap scripts

Prerequisites

- Basic Understanding of Cybersecurity Concepts: Familiarity with fundamental cybersecurity principles and terminology.
- Basic Understanding of the Penetration Testing Lifecycle and methodology.
- Knowledge of Network and Application Security: Understanding of network protocols, architecture, and common security practices.
- Basic Familiarity with Security Tools: Experience using security tools such as Nessus, Nmap, and Wireshark.

Learning Objectives/Outcomes:

- Perform comprehensive network enumeration using Nmap to identify live hosts, open ports, and services running on a target network.
- Effectively leverage the Nmap Scripting Engine (NSE) to perform automated and custom tasks such as vulnerability detection, service version detection, and advanced reconnaissance.
- Analyze and interpret the results of Nmap scans to extract valuable information for penetration testing, including identifying potential attack vectors and vulnerabilities.
- Seamlessly incorporate Nmap and its scripting engine into the penetration testing process, from initial reconnaissance to post-exploitation activities.

Let’s Get Started!

Introduction To Enumeration

Enumeration

- After the host discovery and port scanning phase of a penetration test, the next logical phase is going to involve service enumeration.

- The goal of service enumeration is to gather additional, more specific/detailed information about the hosts/systems on a network and the services running on said hosts.

- This includes information like account names, shares, misconfigured services and so on.

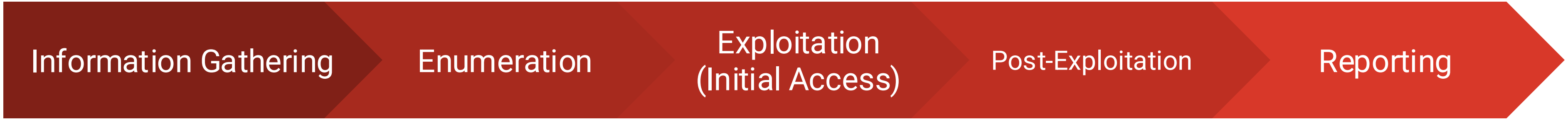
- Like the scanning phase, enumeration involves active connections to the remote devices in the network.

Enumeration

- There are many protocols on networked systems that an attacker can target if they have been misconfigured or have been left enabled.

- In this section of the course, we will be exploring the various tools and techniques that can be used to interact with these protocols, with the intent of eventually/potentially exploiting them in later phases.

Penetration Testing Methodology



Information Gathering

Enumeration

Exploitation
(Initial Access)

Post-Exploitation

Reporting

Passive Information Gathering

OSINT

Active Information Gathering

Network Mapping
Host Discovery
Port Scanning
Service Detection & OS Detection

Service & OS Enumeration

Service Enumeration
User Enumeration
Share Enumeration

Vulnerability analysis and threat modeling

Vulnerability Analysis
Vulnerability Identification

Exploitation

Developing/Modifying Exploits
Service Exploitation

Post Exploitation

Local Enumeration
Privilege Escalation
Credential Access
Persistence
Defense Evasion
Lateral Movement

Reporting

Report Writing
Recommendations

Port Scanning & Enumeration With Nmap

Port Scanning & Enumeration With Nmap

- Nmap is a free and open-source network scanner that can be used to discover hosts on a network as well as scan targets for open ports.

- It can also be used to enumerate the services running on open ports as well as the operating system running on the target system.

- We can output the results of our Nmap scan in to a format that can be imported into MSF for vulnerability detection and exploitation.

Demo: Port Scanning & Enumeration With Nmap

Importing Nmap Scan Results Into MSF

Port Scanning With Auxiliary Modules

Auxiliary Modules

- Auxiliary modules are used to perform functionality like scanning, discovery and fuzzing.

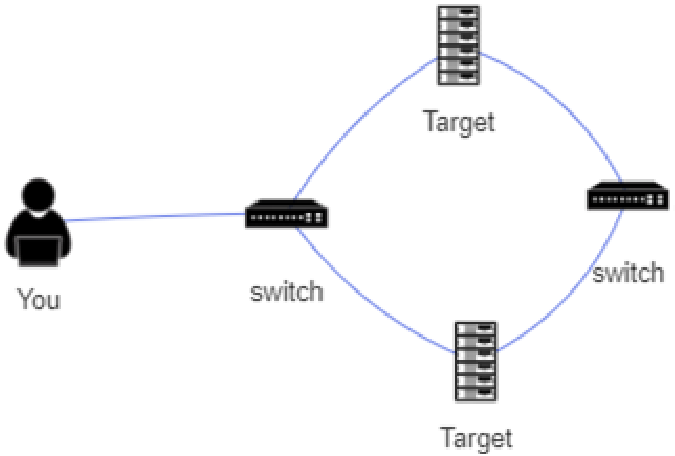
- We can use auxiliary modules to perform both TCP & UDP port scanning as well as enumerating information from services like FTP, SSH, HTTP etc.

- Auxiliary modules can be used during the information gathering phase of a penetration test as well as the post exploitation phase.

- We can also use auxiliary modules to discover hosts and perform port scanning on a different network subnet after we have obtained initial access on a target system.

Lab Infrastructure

- Our objective is to utilize auxiliary modules to discover open ports on our first target.
- The next step will involve exploiting the service running on the target in order to obtain a foothold.
- We will then utilize our foothold to access other systems on a different network subnet (pivoting).
- We will then utilize auxiliary modules to scan for open ports on the second target.



Demo: Port Scanning With Auxiliary Modules

FTP Enumeration

FTP Enumeration

- FTP (File Transfer Protocol) is a protocol that uses TCP port 21 and is used to facilitate file sharing between a server and client/clients.

- It is also frequently used as a means of transferring files to and from the directory of a web server.

- We can use multiple auxiliary modules to enumerate information as well as perform brute-force attacks on targets running an FTP server.

- FTP authentication utilizes a username and password combination, however, in some cases an improperly configured FTP server can be logged into anonymously.

Demo: FTP Enumeration

SMB Enumeration

SMB Enumeration

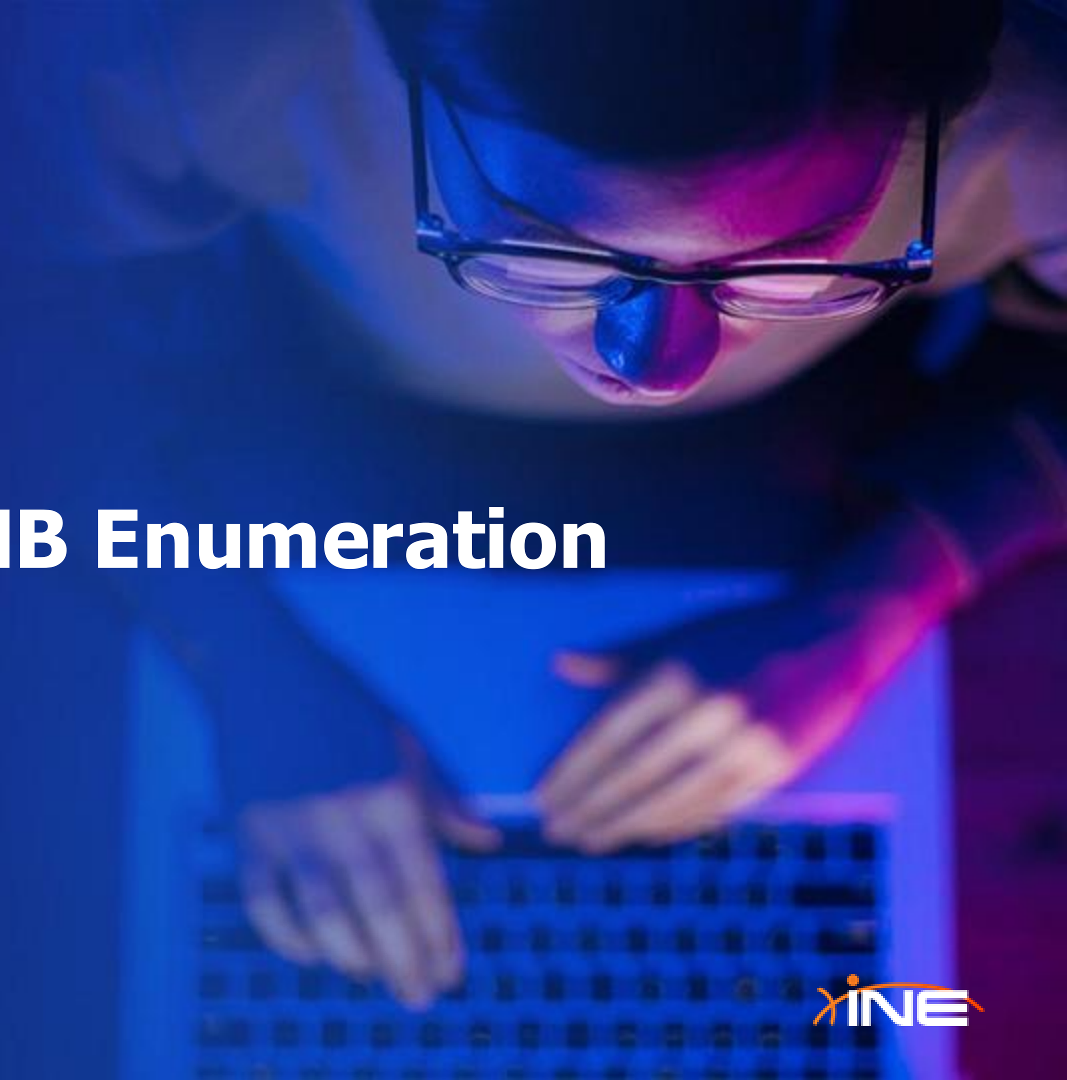
- SMB (Server Message Block) is a network file sharing protocol that is used to facilitate the sharing of files and peripherals between computers on a local network (LAN).

- SMB uses port 445 (TCP). However, originally, SMB ran on top of NetBIOS using port 139.

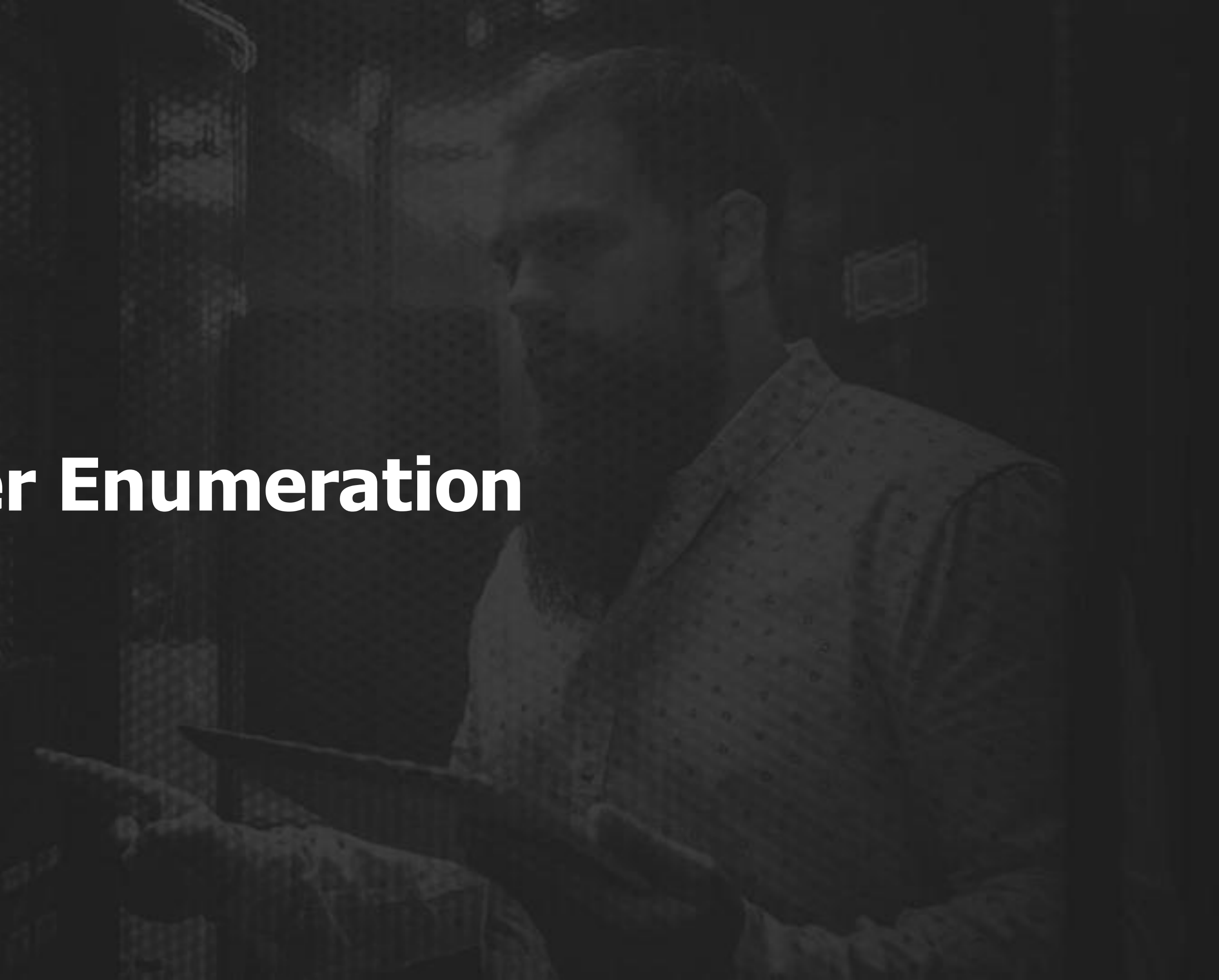
- SAMBA is the Linux implementation of SMB, and allows Windows systems to access Linux shares and devices.

- We can utilize auxiliary modules to enumerate the SMB version, shares, users and perform a brute-force attack in order to identify users and passwords.

Demo: SMB Enumeration



Web Server Enumeration



Web Server Enumeration

- A web server is software that is used to serve website data on the web.
- Web servers utilize HTTP (Hypertext Transfer Protocol) to facilitate the communication between clients and the web server.
- HTTP is an application layer protocol that utilizes TCP port 80 for communication.
- We can utilize auxiliary modules to enumerate the web server version, HTTP headers, brute-force directories and much more.
- Examples of popular web servers are; Apache, Nginx and Microsoft IIS.

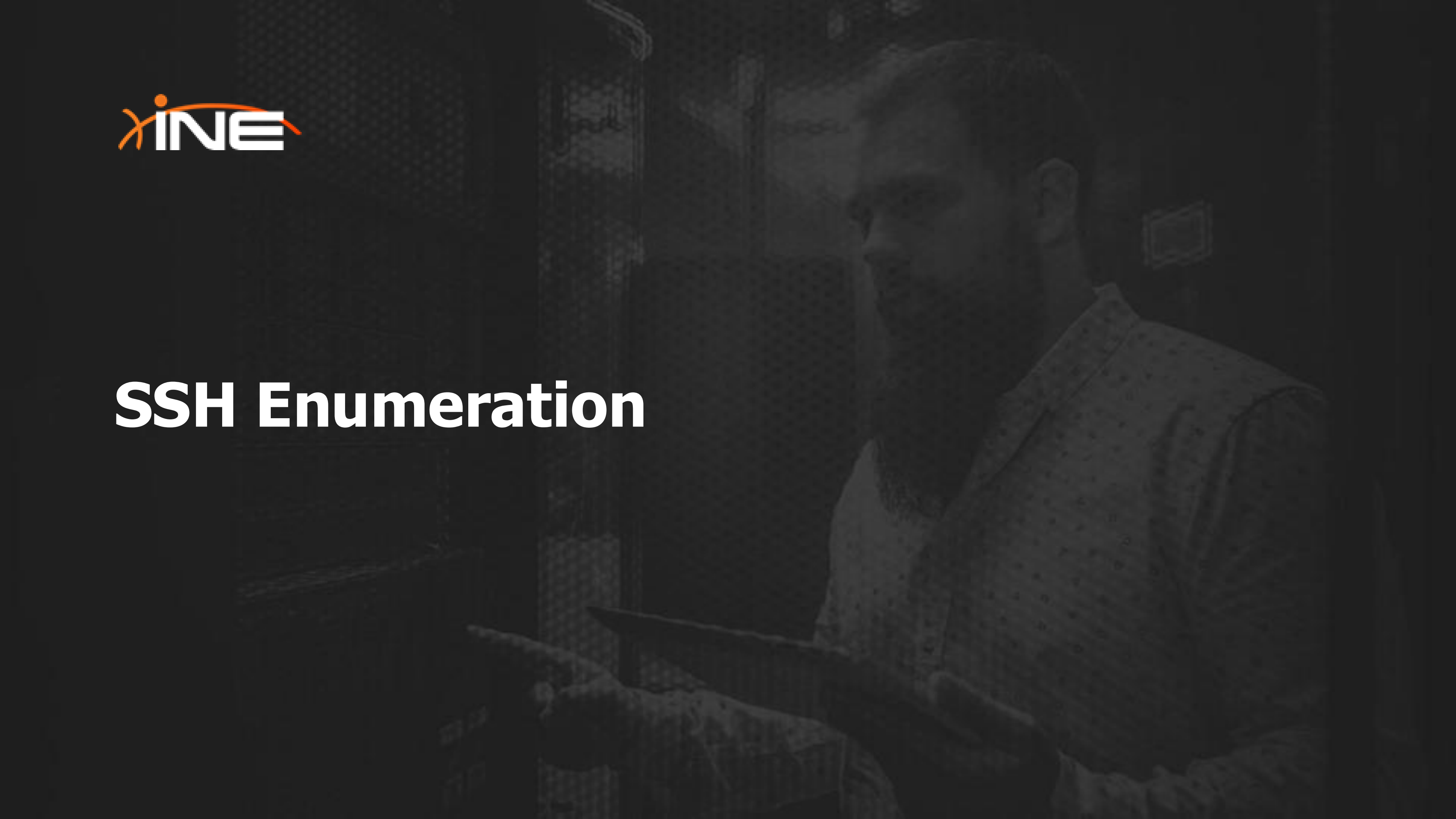
Demo: Web Server Enumeration

MySQL Enumeration

MySQL Enumeration

- MySQL is an open-source relational database management system based on SQL (Structured Query Language).
- It is typically used to store records, customer data, and is most commonly deployed to store web application data.
- MySQL utilizes TCP port 3306 by default, however, like any service it can be hosted on any open TCP port.
- We can utilize auxiliary modules to enumerate the version of MySQL, perform brute-force attacks to identify passwords, execute SQL queries and much more.

Demo: MySQL Enumeration



SSH Enumeration

SSH Enumeration

- SSH (Secure Shell) is a remote administration protocol that offers encryption and is the successor to Telnet.
- It is typically used for remote access to servers and systems.
- SSH uses TCP port 22 by default, however, like other services, it can be configured to use any other open TCP port.
- We can utilize auxiliary modules to enumerate the version of SSH running on the target as well as perform brute-force attacks to identify passwords that can consequently provide us remote access to a target.

Demo: SSH Enumeration

SMTP Enumeration

SMTP Enumeration

- SMTP (Simple Mail Transfer Protocol) is a communication protocol that is used for the transmission of email.

- SMTP uses TCP port 25 by default. It is can also be configured to run on TCP port 465 and 587.

- We can utilize auxiliary modules to enumerate the version of SMTP as well as user accounts on the target system.

Demo: SMTP Enumeration

Enumeration

Course Conclusion

Learning Objectives/Outcomes:

- Perform comprehensive network enumeration using Nmap to identify live hosts, open ports, and services running on a target network.
- Effectively leverage the Nmap Scripting Engine (NSE) to perform automated and custom tasks such as vulnerability detection, service version detection, and advanced reconnaissance.
- Analyze and interpret the results of Nmap scans to extract valuable information for penetration testing, including identifying potential attack vectors and vulnerabilities.
- Seamlessly incorporate Nmap and its scripting engine into the penetration testing process, from initial reconnaissance to post-exploitation activities.

EXPERTS AT MAKING YOU AN EXPERT

INE